ROBERT AHDOOT (SBN 172098)
rahdoot@ahdootwolfson.com
TINA WOLFSON (SBN 174806)
twolfson@ahdootwolfson.com
ALYSSA BROWN (SBN 301313)
abrown@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

Attorneys for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

STACY PENNING, individually and on behalf of all others similarly situated, Plaintiff, v. AT&T INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Stacy Penning ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), upon personal knowledge of facts pertaining to themselves and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendant AT&T Inc. ("AT&T" or "Defendant"), seeking monetary damages, restitution, and/or injunctive relief for the proposed Class Members, as defined below.

NATURE OF THE ACTION

1. Plaintiff brings this class action individually and on behalf of all other individuals who had their sensitive personal information ("Personal Information") disclosed to unauthorized third parties during a data breach compromising AT&T, identified in early 2024 (the "Data Breach").

2. On March 30, 2024, AT&T released an announcement on its website, stating, "AT&T[] has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago."[1]

3. The March 30 announcement went on to state that the data set includes "personal information such as social security numbers, […]."

4. In the same announcement, AT&T disclosed that "[b]ased on our preliminary analysis, the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders."

5. AT&T notified the California Attorney General's Office of the Data Breach sometime after March 26, 2024. AT&T included in its submission a Notice of Data Breach template to be sent out to consumers. In this notice template, AT&T states, "[o]n March 26, 2024, we determined that AT&T customer information was included in a dataset released on the dark web on March 17, 2024."[2]

6. Regarding the types of information disclosed, the notice template reads: "[t]he information varied by individual and account, but may have included full name, email address, mailing

[1] AT&T Addresses Recent Data Set Released on the Dark Web, https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed on May 2, 2024).

[2] Customer Notification Letter Template; Notice of Data Breach, https://oag.ca.gov/system/files/Customer%20Notification%20Letter%20Template.pdf (last accessed on May 2, 2024).

address, phone number, social security number, date of birth, AT&T account number and AT&T passcode."

7. Though AT&T claims in that same letter that "we are committed to keeping your information secure," it concedes that the data set involved in the Data Breach was likely from 2019. AT&T provides no explanation as to why it still maintained Personal Information in its systems for 65.4 million individuals who are no longer AT&T customers, and who may not have been customers for nearly five years.

8. AT&T was aware, or should have known, its data security shortcomings. It collects and maintains sensitive Personal Information about its customers and potential customers, including Social Security numbers ("SSNs") and financial information. It requires customers to provide this information in connection with using its services.

9. Putting aside that large companies that collect sensitive Personal Information are routinely breached and that AT&T is aware of this, AT&T itself suffered a prior data breach in March 2023, which also exposed customer data.[3]

10. Despite this history of data incidents, AT&T failed to make necessary changes to implement industry standard data privacy measures, exposing its customers, and former customers, to the risk of being impacted by a breach.

11. AT&T also evidently took no steps to delete or minimize Personal Information it no longer needed for its regular course of business, including the Personal Information for individuals who were former AT&T customers.

12. AT&T's failures to ensure that its servers and systems were adequately secure fell far short of its obligations and Plaintiff's and Class Members' reasonable expectations for data privacy, jeopardized the security of Plaintiff's and Class Member's Personal Information, and exposed Plaintiff and Class Members to fraud and identity theft or the serious risk of fraud and identity theft.

13. As a result of Defendant's conduct and the resulting Data Breach, Plaintiff and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, they

[3] In March 2023, AT&T notified 9 million wireless customers that their customer proprietary network information (CPNI) was compromised in a data breach at a third-party vendor.

have either suffered fraud or identity theft, or face an imminent and ongoing risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

PARTIES

14. Stacy Penning is an adult citizen of the state of California and resides in El Cerrito, California. Penning is a current customer of AT&T. Believing AT&T would implement and maintain reasonable security and practices to protect customer Personal Information, Penning provided Personal Information to AT&T in connection with seeking telecommunications services from, and transacting with, AT&T.

15. Penning would not have entrusted his Personal Information to AT&T had he known that AT&T would fail to adequately safeguard such information.

16. Penning received a letter from AT&T, notifying him of the data breach in early April, 2024.

17. Defendant AT&T, Inc. is a corporation organized under the laws of the state of Delaware, with a principal place of business located in Dallas, Texas. AT&T serves customers nationwide, with a concentration in 21 states, including California.[4] AT&T has offices throughout the nation, including in the Northern District of California.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), there are in excess of 100 Class Members, the action is a class action in which one or more Class Members are citizens of states different from Defendant, and Defendant is not a government entity.

19. The Court has personal jurisdiction over AT&T because AT&T has committed acts within this District giving rise to this action, conducts significant business in California, has offices throughout California, and otherwise has sufficient minimum contacts with and intentionally avails itself

[4] Key AT&T U.S. Service Regions; https://www.att.com/Common/merger/files/pdf/att-us-service-area-map-21-state.pdf (last accessed on May 2, 2024).

of the markets in California. AT&T has engaged in continuous, systematic, and substantial activities within the state, including marketing and sales of the services connected to the data breach. AT&T's legal department also has offices in the Northern District of California (San Francisco, CA).

20. Venue properly lies in this judicial district because, *inter alia,* AT&T transacts substantial business, has agents, and is otherwise located in this district; a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district; and Plaintiff is domiciled in this district.

FACTUAL ALLEGATIONS

A. AT&T Collects and Stores Personal Information

21. AT&T routinely collects sensitive Personal Information in the process of providing its services and products, which include telecommunications services, such as wired and wireless telephone services, fiber optics, internet, and other means of transmitted communications.

22. This Personal Information includes, on information and belief, standard "phone book" information such as names, email addresses, phone numbers, mailing addresses, but also includes highly sensitive information including SSNs, financial information, and date of birth.

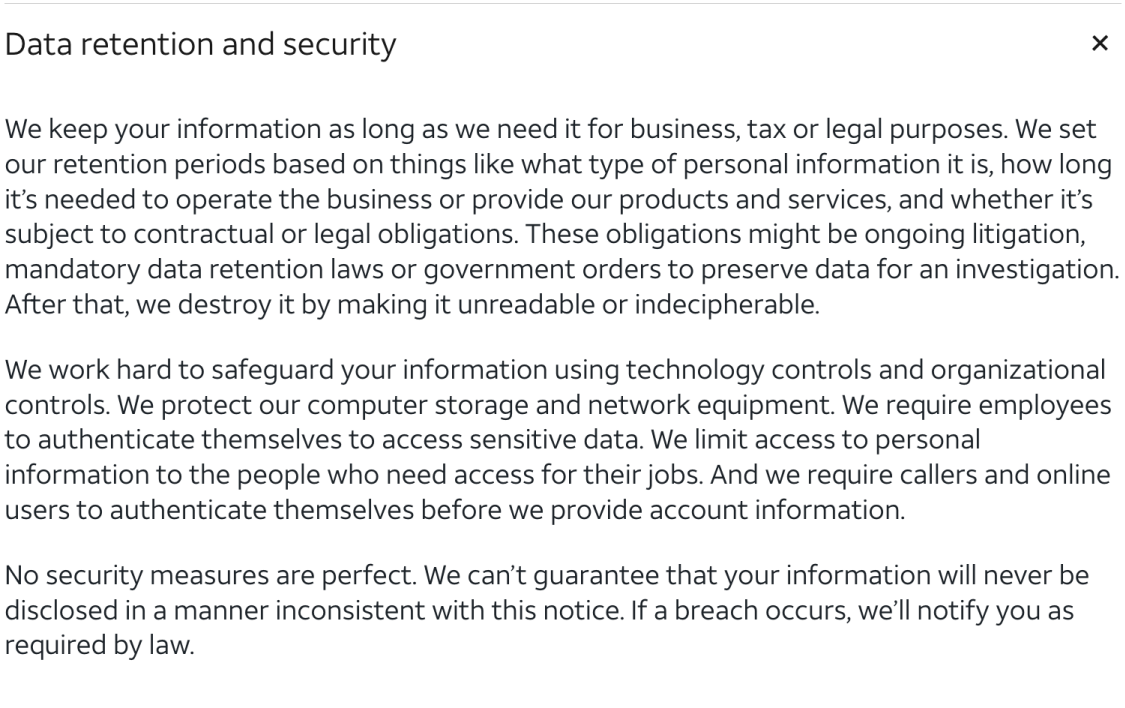
23. Defendant is and was aware of the sensitive nature of the Personal Information it collects, and it acknowledges the importance of data privacy. On its Privacy Center on its website, AT&T states, "[y]ou can count on us to provide you with products and services designed with privacy in mind, while also giving you control over how your information is shared."[5]

24. The Privacy Center also states, "[w]e use strong safeguards to keep your data safe and secure."[6]

[5] AT&T Privacy Center, https://about.att.com/privacy.html (last accessed on May 2, 2024).

[6] *Id.*

25. Regarding data retention, AT&T's website indicates[7]:



Data retention and security ×

We keep your information as long as we need it for business, tax or legal purposes. We set our retention periods based on things like what type of personal information it is, how long it's needed to operate the business or provide our products and services, and whether it's subject to contractual or legal obligations. These obligations might be ongoing litigation, mandatory data retention laws or government orders to preserve data for an investigation. After that, we destroy it by making it unreadable or indecipherable.

We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.

No security measures are perfect. We can't guarantee that your information will never be disclosed in a manner inconsistent with this notice. If a breach occurs, we'll notify you as required by law.

[7] AT&T Privacy Center, https://about.att.com/privacy/privacy-notice.html#data-retention (last accessed on May 2, 2024).

26. AT&T's website provides a chart that shows how they utilize certain Personal Information. The chart includes the following, indicating that it uses SSNs and other Personal Information for credit reporting and fraud prevention[8]:

Categories	Purpose for collection	Categories of companies we've shared with	Purpose for sharing (making available constitutes a share)
Gov't IDs: Social Security, driver's license, state Identification card, or passport number	• Provide information to or receive information from credit reporting agencies • Prevent fraud/authenticate identity	• Cloud storage companies • Credit reporting agencies • Fraud prevention and authentication/identity verification entities	• Report to or receive information from credit reporting agencies • Prevent fraud /provide identity verification

27. Based on the information that can be found in AT&T's Privacy Center, it is clear that AT&T was aware of the need to safeguard the sensitive Personal Information entrusted to it by consumers, and had policies in place to ensure the deletion of Personal Information that was no longer required. What is not clear is why these policies were not followed.

B. <u>The Data Breach</u>

28. In or about March 17, 2024, a threat actor accessed AT&T's systems, gaining access to Plaintiff and Class Members' sensitive Personal Information.

[8] AT&T Privacy Center, https://about.att.com/privacy/privacy-notice/state-disclosures.html#sensitive-personal-info (last accessed on May 2, 2024).

29. On or about March 30, 2024, AT&T disclosed the Data Breach on its website. AT&T disclosed the following[9]:

> AT&T* has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago. While AT&T has made this determination, it is not yet known whether the data in those fields originated from AT&T or one of its vendors. With respect to the balance of the data set, which includes personal information such as social security numbers, the source of the data is still being assessed.
>
> AT&T has launched a robust investigation supported by internal and external cybersecurity experts. Based on our preliminary analysis, the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders.

30. On April 12, 2024, AT&T added a page to its website regarding the Data Breach, entitled "Keeping your account secure." On that page, AT&T indicates that they have reset account passwords for an extra layer of protection, are emailing or mailing letters to individuals with compromised sensitive personal information, and offering identity theft and credit monitoring services.[10]

31. Despite the webpage acknowledging that the data set "appears to be from 2019 or earlier," AT&T states that it is "reaching out to all 7.6M impacted *customers*," (emphasis added). AT&T made no indication on this particular webpage that it would be notifying the 65.4 million former customers.

32. On information and belief, this Data Breach is not the first time that AT&T has failed to protect its customers' Personal Information. In 2021, a very similar dataset was offered for sale by a

[9] AT&T Addresses Recent Data Set Released on the Dark Web, https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed on May 2, 2024).

[10] Keeping your account secure, https://www.att.com/support/article/my-account/000101995?source=ESsWCfCTA0000000L&wtExtndSource=cfm_accountsafety_thread (last accessed on May 2, 2024).

group known as ShinyHunters for $1 million. At the time, AT&T denied that the information originated from its systems.[11]

33. On or around August 12, 2022, AT&T also denied any connection to a database found on the dark web that included the Social Security Numbers of 23 million Americans, despite the cybersecurity company who discovered the database indicating there was evidence tying the database to AT&T.[12]

34. On or around March 9, 2023, AT&T also confirmed a data breach had affected 9 million of its customers, but denied that its own systems were compromised.[13]

C. Impact of the AT&T Data Breach

35. The actual extent and scope, and the impact, of the Data Breach on AT&T's customers (and former customers) remains uncertain. Unfortunately for Plaintiff and Class Members, the damage is already done because their sensitive Personal Information is confirmed by AT&T to have been disclosed to unauthorized persons during the Data Breach.

36. AT&T knew or should have known that its affected IT systems and/or servers are unsecure and do not meet industry standards for protecting highly sensitive customer Personal Information. On information and belief, AT&T failed to timely make changes to its data security systems, privacy policies, and its IT systems and servers, exposing its customers' Personal Information to the risk of theft, identity theft, and fraud.

37. AT&T's representation that the data set likely came from 2019 or before indicates one of two possibilities: (1) that AT&T improperly retains highly sensitive Personal Information for former customers for up to five years following their disengagement with AT&T; or (2) that the data set was obtained from AT&T at some point up to five years ago (including, but not limited to the 2021, 2022, or 2023 breaches outlined above), with no notice to consumers until March 2024.

---

[11] Jonathan Greig, *AT&T confirms legitimacy of leak involving information of 73 million people*, THE RECORD (Apr. 1, 2024), https://therecord.media/att-confirms-data-leak-73-million-people.

[12] Jonathan Greig, *AT&T denies connection to database of 23 million SSNs, says it may be tied to credit agency breach*, THE RECORD (Aug. 12, 2022), https://therecord.media/att-denies-connection-to-database-of-23-million-ssns-says-it-may-be-tied-to-credit-agency-breach.

[13] Jonathan Greig, *AT&T says 9 million customers exposed in January vendor breach*, THE RECORD (Mar. 10, 2023), https://therecord.media/att-says-nine-million-exposed-in-data-breach.

38. The harm caused to Plaintiff and Class Members by the Data Breach has already been suffered.

39. The Data Breach creates a heightened security concern for Plaintiff and Class Members because their SSNs and other sensitive information was disclosed. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of his SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

40. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[14] TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[15]

41. AT&T had a duty to keep Plaintiff's and Class Members' Personal Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their Personal Information to AT&T with the understanding that AT&T would comply with its own privacy policies and its obligations to keep such information confidential and secure from unauthorized disclosures.

42. Defendant's data security obligations were particularly important given the substantial increase in data breaches in recent years, which are widely known to the public and to anyone in AT&T's industry.

D. Theft of Personal Information Has Serious Consequences for Victims

43. Data breaches are by no means new, and they should not be unexpected. Business Insider

[14] *Fact Sheet: The Work of the President's Identity Theft Task Force*, U.S. DEP'T OF JUSTICE (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html.

[15] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

has noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[16] It is well known amongst companies that store sensitive personally identifying information that sensitive Personal Information—like SSNs, financial information, tax information, etc.—is valuable and frequently targeted by criminals.

44. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, like AT&T, and these companies must ensure that data privacy and security practices and protocols are adequate to protect against and prevent known and expected attacks.

45. Theft of Personal Information is serious. The Federal Trade Commission has warned consumers that identity thieves use Personal Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[17]

46. Indeed, with access to an individual's Personal Information, criminals can do more than simply empty a victim's bank account. They can also commit all manner of fraud, including: obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; obtain lending or lines of credit; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[18]

47. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write

[16] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[17] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed May 2, 2024).

[18] *See* FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed May 2, 2024).

bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[19]

48. Personal Information is a valuable property right.[20] The value of sensitive personal information as a commodity is measurable.[21] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[22]

49. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs, financial information, driver's license numbers, and other Personal Information directly on various illegal websites making the information publicly available, often for a price. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

50. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

51. Consumers place a high value on the privacy of sensitive data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm

---

[19] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[20] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[21] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[22] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[23]

52. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[24]

53. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Personal Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

54. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[25]

55. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. AT&T Failed to Act in the Face of a Known Risk of a Data Breach

56. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Defendant failed to take reasonable steps to adequately protect Personal Information, leaving its clients (and potentially others) exposed to risk of fraud and identity theft.

57. AT&T is, and at all relevant times has been, aware that the sensitive Personal Information it handles and stores in connection with providing lending services and products is highly sensitive. As

---

[23] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[24] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[25] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

a company that requires highly sensitive and identifying information in connection with providing its products and services, AT&T is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

58. AT&T was aware, or should have been aware, of regulatory and industry guidance regarding data security, and was alerted to the risk associated with failing to ensure that Personal Information was adequately secured.

59. Despite the well-known risks of hackers and cybersecurity intrusions, Defendant failed to employ adequate data security measures in a meaningful way in order to prevent breaches, including the Data Breach.

60. The security flaws inherent to Defendant's IT systems or servers run afoul of industry best practices and standards. Had Defendant adequately protected and secured its servers or systems, and the sensitive Personal Information stored therein, it could have prevented the Data Breach.

61. Despite that AT&T was on notice of the very real possibility of data theft, including through a prior data breach, it still failed to make necessary changes, and permitted a massive intrusion to occur that resulted in disclosure of Plaintiff's and nearly 73 million other Class Members' Personal Information to criminals.

62. Defendant permitted Class Members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

63. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with industry data security standards.[26]

64. As a result of the events detailed herein, Plaintiff and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value

[26] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 30, 2017), https://www.reuters.com/article/idUSKBN18M2BY/.

and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

65. Victims of the Data Breach have likely already experienced harms and are subject to an imminent and ongoing risk of harm, including identity theft and fraud.

66. As a result of AT&T's failure to ensure that its impacted systems and servers were protected and secured, the Data Breach occurred. As a result of the Data Breach, Plaintiff's and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

CLASS ALLEGATIONS

67. Plaintiff brings this action on behalf of himself and the following Classes pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**
> All residents of the United States who were impacted by the AT&T Data Breach, including all persons who were sent notice by AT&T that their Personal Information was compromised as a result of the Data Breach.
>
> **California Class**
> All residents of the state of California who were impacted by the AT&T Data Breach, including all persons who were sent notice by AT&T that their Personal Information was compromised as a result of the Data Breach.

68. Excluded from the Class are: (1) any Judge presiding over this action, members of their immediate families, and Court Staff; and (2) AT&T, its subsidiaries, parent companies, successors, predecessors, and any entity in which AT&T, or its parents, have a controlling interest, and its current or former officers and directors.

69. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Classes are so numerous that their individual joinder is impracticable, as the proposed Class(es) appear to include many millions of members who are geographically dispersed.

70. **Typicality**: Plaintiff's claims are typical of Class Members' claims. Plaintiff and all Class Members were injured through Defendant's uniform misconduct, and Plaintiff's claims are

identical to the claims of the Class Members they seek to represent. Accordingly, Plaintiff's claims are typical of Class Members' claims.

71. **Adequacy**: Plaintiff's interests are aligned with the Class(es) Plaintiff seeks to represent, and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and undersigned counsel intend to prosecute this action vigorously. The Class(es)' interests are well-represented by Plaintiff and undersigned counsel.

72. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class member's claims. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

73. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

- whether Defendant engaged in the wrongful conduct alleged herein;
- whether Defendant's data security practices resulted in the disclosure of Plaintiff's and other Class Members' Personal Information and the Data Breach;
- whether Defendant violated privacy rights and invaded Plaintiff's and Class Members' privacy; and
- whether Plaintiff and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

74. Given that Defendant engaged in a common course of conduct as to Plaintiff and the Classes, similar or identical injuries and common law and statutory violations are involved, and common

questions outweigh any potential individual questions.

75. **Injunctive and Declaratory Relief:** Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CAUSES OF ACTION

COUNT I
Negligence

76. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

77. Defendant was entrusted with, stored, and otherwise had access to the Personal Information of Plaintiff and Class Members.

78. Defendant knew, or should have known, of the risks inherent to storing the Personal Information of Plaintiff and Class Members, and to not ensuring that its servers and systems, and the Personal Information, was secure. These risks were reasonably foreseeable to Defendant, including because Defendant has previously experienced a data breach.

79. Defendant owed duties of care to Plaintiff and Class Members whose Personal Information had been entrusted to it.

80. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate data security. Defendant had a duty to safeguard Plaintiff's and Class Members' Personal Information and to ensure that their adequately protected Personal Information. Defendant breached this duty.

81. Defendant further breached its duties by failing to detect the Data Breach in a timely manner and failing to disclose to consumers that its security practices were not sufficient to protect Plaintiff's and Class Members' Personal Information.

82. AT&T's duty of care arises from its knowledge that its customers entrust it with highly sensitive Personal Information that AT&T is required to, and represents that it will, handle securely. Indeed, on its website, AT&T commits to data privacy in its Privacy Center, including safeguarding sensitive Personal Information.

83. Only AT&T was in a position to ensure that its systems, servers, and services were sufficient to protect against breaches and the harms that Plaintiff and Class Members have now suffered.

84. A "special relationship" exists between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. Defendant entered into a "special relationship" with Plaintiff and Class Members by agreeing to accept, store, and have access to sensitive Personal Information provided by Plaintiff and Class Members in connection with their attempts or efforts to secure lending.

85. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

86. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' Personal Information.

87. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known it was failing to meet these duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

88. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have been harmed and face an imminent and ongoing risk of harm.

89. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se

90. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

91. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), AT&T had a duty to provide adequate data security practices in connection with safeguarding Plaintiff's and Class Members' Personal Information.

92. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), AT&T had a duty to provide adequate data security practices to safeguard Plaintiff's and Class Members' Personal Information.

93. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA"), Cal. Civ. Code §§ 1798.80, *et seq.*, among other statutes, by failing to provide fair, reasonable, or adequate data security in connection with the sale of lending products and services in order to safeguard Plaintiff's and Class Members' Personal Information.

94. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

95. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

96. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known that it was failing to meet its duties, and that a breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

97. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Class Members have been harmed and face an imminent and ongoing risk of harm.

98. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract

99. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

100. AT&T either currently provides or previously provided various telecommunications services to Plaintiff and Class Members.

101. In connection with their business relationship, Plaintiff and Class Members entered into implied contracts with AT&T.

102. Pursuant to these implied contracts, Plaintiff and Class Members provided AT&T with their Personal Information. In exchange, AT&T agreed, among other things: (1) to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Personal

Information; and (2) to protect Plaintiff's and Class Members' Personal Information in compliance with federal and state laws and regulations and industry standards.

103. The protection of Personal Information was a material term of the implied contracts between Plaintiff and Class Members, on the one hand, and AT&T, on the other hand. Had Plaintiff and Class Members known that AT&T would not adequately protect its customers' Personal Information they would not have done business with AT&T.

104. Plaintiff and Class Members performed their obligations under the implied contract when they provided AT&T with their Personal Information.

105. Necessarily implicit in the agreements between Plaintiff/Class Members and AT&T was AT&T's obligation to take reasonable steps to secure and safeguard Plaintiff's and Class Members' Personal Information.

106. AT&T breached its obligations under its implied contracts with Plaintiff and Class Members by failing to implement and maintain reasonable security measures to protect their Personal Information.

107. AT&T's breach of its obligations of its implied contracts with Plaintiff and Class Members directly resulted in the Data Breach.

108. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of AT&T's material breaches of its agreements.

109. Plaintiff and other Class Members were damaged by AT&T's breach of implied contracts because: (i) they have suffered actual harm or identity theft; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Personal Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Personal Information has been breached; (v) they were deprived of the value of their Personal Information, for which there is a well-established national and international market; (vi) they were deprived of the benefit of their bargain; and/or (vii) they lost time and money incurred to mitigate and remediate the effects of the breach, including the increased risks of identity theft they face and will continue to face.

COUNT IV
Breach of Fiduciary Duty

110. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

111. A relationship existed between Plaintiff and Class Members and Defendant in which Plaintiff and Class Members put their trust in Defendant to protect the Personal Information of Plaintiff and Class Members and Defendant accepted that trust.

112. Defendant breached the fiduciary duties that they owed to Plaintiff and Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the Personal Information of Plaintiff and Class Members.

113. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and Class Members.

114. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

115. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class Members.

116. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff are entitled to and demand actual, consequential, and nominal damages, and injunctive relief.

COUNT V
Violations of the California Customer Records Act
Cal. Civ. Code §§ 1798.80, *et seq.* ("CCRA")

117. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

118. This claim is pleaded on behalf of Plaintiff and the California class.

119. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

120. By failing to implement reasonable measures to protect Plaintiff's Personal Information, Defendants violated Civil Code § 1798.81.5.

121. In addition, by failing to promptly notify all affected Class Members that their Personal Information had been exposed, Defendant violated Civil Code § 1798.82.

122. As a direct or proximate result of Defendant's violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiff and California Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages and harms described herein.

123. In addition, by violating Civil Code §§ 1798.81.5 and 1798.82, Defendant "may be enjoined" under Civil Code Section 1798.84(e).

124. Defendant's violations of Civil Code §§ 1798.81.5 and 1798.82 also constitute unlawful acts or practices under the UCL, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

125. Plaintiff accordingly requests that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendant utilize strong industry standard data security measures for the collection, storage, and retention of customer data; (2) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (3) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures; (5) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendant purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (7) ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendant, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive

Personal Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their Personal Information.

126. Plaintiff further requests that the Court require Defendant AT&T to identify and notify all members of the Class who have not yet been informed of the Data Breach, and to notify affected persons of any future data breaches by email within 24 hours of discovery of a breach or possible breach and by mail within 72 hours.

COUNT VI
Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL")

127. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

128. This claim is pleaded on behalf of Plaintiff and the California class.

129. Defendant engaged in unfair, unlawful, and fraudulent business practices in violation of the UCL.

130. Plaintiff suffered injury in fact and lost money or property as a result of Defendant's alleged violations of the UCL.

131. The acts, omissions, and conduct of Defendant as alleged constitute a "business practice" within the meaning of the UCL.

Unlawful Prong

132. Defendant violated the unlawful prong of the UCL by violating, without limitation, the CCPA, CCRA, and FTC Act as alleged herein.

133. Defendant AT&T violated the unlawful prong of the UCL by failing to honor the terms of its implied contracts with Plaintiff and Class Members in California, as alleged herein.

134. Defendant's conduct also undermines California public policy—as reflected in statutes like the California Information Practices Act, Cal. Civ. Code §§ 1798, *et seq.*, the CCPA concerning consumer privacy, and the CCRA concerning customer records—which seek to protect customer and

consumer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

Unfair Prong

135. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because Defendant's acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other Class Members in California. The gravity of Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

136. Defendant's failure to utilize, and to disclose that they do not utilize, industry standard security practices, constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to the Class. While Defendant's competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Defendant has not—to the detriment of its customers and to competition.

Fraudulent Prong

137. By failing to disclose that it does not enlist industry standard security practices, all of which rendered Class Members particularly vulnerable to data breaches, Defendant AT&T engaged in UCL-violative practices.

138. A reasonable consumer would not have transacted with AT&T if they knew the truth about its security procedures. By withholding material information about its security practices, AT&T was able to obtain customers who provided and entrusted their Personal Information in connection with transacting business with AT&T. Had Plaintiff known the truth about AT&T's security procedures, Plaintiff would not have done business with AT&T.

139. As a result of Defendant's violations of the UCL, Plaintiff and Class Members in California are entitled to injunctive relief including, but not limited to: (1) ordering that Defendant utilize strong industry standard data security measures for the collection, storage, and retention of customer data; (2) ordering that Defendant, consistent with industry standard practices, engage third party security

auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (3) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures; (5) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendant purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (7) ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendant, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Personal Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their Personal Information.

140. As a result of Defendant's violations of the UCL, Plaintiff and Class Members have suffered injury in fact and lost money or property, as detailed herein. They agreed to transact business with AT&T or made purchases or spent money that they otherwise would not have made or spent, had they known the truth. Class Members lost Personal Information, which is their property. Class Members lost money as a result of dealing with the fallout of and attempting mitigate harm arising from the Data Breach.

141. Plaintiff requests that the Court issue sufficient equitable relief to restore Class Members in California to the position they would have been in had Defendant not engaged in violations of the UCL, including by ordering restitution of all funds that Defendant may have acquired from Plaintiff and Class Members in California as a result of those violations.

COUNT VII
Invasion of Privacy (Intrusion Upon Seclusion)

142. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

143. Plaintiff and Class Members had a reasonable expectation of privacy in the Personal Information that Defendant disclosed without authorization.

144. By failing to keep Plaintiff's and Class Members' Personal Information safe, knowingly employing inadequate data privacy policies and protocols, and disclosing Personal Information to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy by, *inter alia*:

a. intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. invading Plaintiff's and Class Members' privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure Personal Information from disclosure to unauthorized persons;

d. enabling the disclosure of Plaintiff's and Class Members' Personal Information without consent.

145. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider its actions highly offensive.

146. Defendant knew that its IT systems and servers were vulnerable to data breaches prior to the Data Breach.

147. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by disclosing their Personal Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

148. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiff's and Class Members' protected privacy

interests.

149. In failing to protect Plaintiff's and Class Members' Personal Information, and in disclosing Plaintiff's and Class Members' Personal Information, Defendant acted with malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

150. Plaintiff seeks injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

COUNT VIII
Unjust Enrichment

151. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

152. This claim is pleaded in the alternative to the implied contract claim.

153. AT&T has profited and benefited from the monies or fees paid and the Personal Information provided by Plaintiff and Class Members to receive services from AT&T.

154. AT&T has voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Plaintiff and Class Members did not receive services of the quality, nature, fitness, or value represented by AT&T and that reasonable consumers expected.

155. AT&T has been unjustly enriched by its withholding of and retention of these benefits, at the expense of Plaintiff and Class Members.

156. Equity and justice militate against permitting AT&T to retain these profits and benefits.

157. Plaintiff and Class Members suffered injury as a direct and proximate result of AT&T's unjust enrichment and seek an order directing AT&T to disgorge these benefits and pay restitution to Plaintiff and Class Members.

COUNT VIII
Declaratory Relief

158. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

159. Plaintiff and the Class Members have stated claims against AT&T based on negligence,

negligence per se, and various state statutes.

160. The Data Breach evidences AT&T's failure to provide security measures that were adequate, reasonable, and/or compliant with industry standards and best practices with regard to safeguarding Plaintiff and Class Members' Personal Information.

161. AT&T's history of involvement in the various data breaches outlined above, including the Data Breach at issue, demonstrates that AT&T's systems remain vulnerable to unauthorized access, and more stringent measures must be taken to safeguard the Personal Information of Plaintiffs and the Class Members going forward.

162. An actual controversy has arisen regarding AT&T's current obligations to provide reasonable data security measures to protect the Personal Information of Plaintiffs and Class Members.

163. AT&T has made no indication that they will be implementing better security measures in the wake of the Data Breach.

164. Thus, on information and belief, AT&T maintains that its security measures were, and still are, adequate and denies that they have an obligation to implement better security measures to protect the Personal Information of Plaintiff and the Class Members.

165. Plaintiff seeks a declaration that AT&T's current security measures are inadequate to safeguard Personal Information, do not comply with their obligations to keep Personal Information secure, and that AT&T must implement specific additional security practices to provide reasonable protection and security for the Personal Information it maintains, including the Personal Information of Plaintiff and Class Members.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Classes, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and Class Members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class

Members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiff and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: May 2, 2024

Respectfully submitted,

/s/ Robert Ahdoot

ROBERT AHDOOT (SBN 172098)
rahdoot@ahdootwolfson.com
TINA WOLFSON (SBN 174806)
twolfson@ahdootwolfson.com
ALYSSA BROWN (SBN 301313)
abrown@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

Attorneys for Plaintiff and the Proposed Classes